# PERIOD AND INDEX OF GENUS ONE CURVES OVER NUMBER FIELDS

SHAHED SHARIF

Abstract. The period of a curve is the smallest positive degree of Galois-invariant divisor classes. The index is the smallest positive degree of rational divisors. We construct examples of genus one curves with prescribed period and index over certain number fields.

## 1. Introduction

Let $X$ be a nonsingular, projective, geometrically integral curve over a field $K$. Define the *index* $I(X)$ to be the greatest common divisor of $[L : K]$, where $L$ varies over finite algebraic field extensions for which $X(L) \neq \emptyset$. In particular, if $X$ has a rational point over $K$ already, the index is 1. Define the *period* $P(X)$ of $X$ to be smallest positive degree amongst Galois-invariant divisor classes on $X$. That is, if $\overline{K}$ is an algebraic closure for $K$, then we consider divisor classes on $\overline{X} := X \times \overline{K}$ which are fixed points for the Galois action $\mathrm{Gal}(\overline{K}/K)$. We have $P(X) \mid I(X)$, for the Galois orbit of any $x \in X(L)$ yields an invariant divisor class. However, the two need not be equal: take the example of a conic without rational points, say (the projective curve given by) $x^2 + y^2 = -1$ over $\mathbb{R}$. Clearly, the index is 2, but the class of a single point is Galois invariant.

In [10], Lichtenbaum showed that

**Theorem 1.1.** *For $X/K$ as above, if the genus, period, and index of $X$ are $g$, $P$, and $I$ respectively, then $P \mid I \mid 2P^2$, $I \mid (2g - 2)$, and if either $(2g - 2)/I$ or $P$ is even, then $I \mid P^2$.*

However, over local fields and $C_1$ fields, the above divisibility conditions are not sharp. For example, for genus 1 curves over local fields, the period and index are always equal [10]. One may then ask what triples $(g, P, I)$ actually occur as the genus, period, and index of a curve over a fixed $K$. Over local fields of characteristic not 2, the problem is solved in [18]. We consider the case $g = 1$ and prove the following:

**Theorem 1.2.** *Let $K$ be a number field and $E$ an elliptic curve over $K$. Let $\ell$, $n$ be positive integers such that $\ell \mid n$. Suppose either that $K$ contains the $n$th roots of unity, or that $E$ has an order $n$ Galois-stable cyclic subgroup. If $n$ is even and $4 \nmid \ell$, suppose further that $K$ contains the $(2n)$th roots of unity, or that $E$ has a Galois-stable cyclic subgroup of order $2n$. Then there exists a genus 1 curve $X$ with Jacobian $E$ for which $P(X) = n$ and $I(X) = n\ell$.*

---

*Date*: October 11, 2008.
The author would like to thank Bjorn Poonen and Pete Clark for very helpful conversations.

Note that for $g = 1$, $(2g-2)/I$ is always even; therefore by Theorem 1.1 we have $I \mid P^2$. For $K$ satisfying the hypotheses of Theorem 1.2, then, we have covered every possible period and index for genus 1 curves.

The significance of period and index lies in computations of Tate-Shafarevich and Brauer groups. Grothendieck [7, §4 et seq.] is the canonical source for these computations. Gonzalez-Avilés [6] showed that given a (suitably nice) curve $X$ over a global field $K$, under certain hypotheses the finiteness of the Brauer group of a model for $X$ is equivalent to the finiteness of the Tate-Shafarevich group of the Jacobian of $X$. The relationship between the sizes of these groups is then computable, and depends on the indices and periods of $X$ both over $K$ and over the completions of $K$. Liu, Lorenzini, and Raynaud extended this result ([11, Theorem 4.3] and [12]). They showed that for $K$ the function field of a curve over a finite field, and assuming that for some prime $\ell$ the $\ell$-part of $\operatorname{Br} X$ is finite, or that the Tate-Shafarevich group of the Jacobian of $X$ is finite, we have $\operatorname{Br} X$ is finite and has square order.

Lastly, in a forthcoming paper [4] the author with Pete Clark uses a similar result as the one in this paper to show that if $E$ is an elliptic curve over a number field $K$, $p$ is a prime and $N$ any integer, then there exists a $p$-extension $L/K$ such that $\#Ш(E/L)[p] \geq N$; that is, the order of the $p$-torsion of the Tate-Shafarevich group is unbounded over $p$-extensions.

For other results exhibiting curves with various periods and indices, see Cassels [1], Lang-Tate [8], Stein [20], O'Neil [15], and Clark [2], [3] and [5]. The strongest previous results in this direction are Clark's, who proved that when $E[p] \subset E(K)$ for $p$ prime, there are principal homogeneous spaces for $E$ with period $p$ and index $p^2$, and that there are curves of every index over every number field.

Recently, Jakob Stix [21] has shown that if $X$ is a curve over $\mathbb{Q}$ and there is a section for the canonical map $\pi_1(X) \to \pi_1(\mathbb{Q})$, then the period and index of $X$ are equal.

## 2. Preliminary Results

2.1. **Basic properties of period and index.** One can alternatively define the index to be the smallest positive degree of a divisor on $X$ over $K$. If $x \in X(\overline{K})$, the Galois orbit of $x$ written as a divisor $\sum({}^\sigma x)$ furnishes a rational divisor of positive degree. Any prime divisor (of $\operatorname{Div} X$, not $\operatorname{Div} \overline{X}$) is necessarily of this form. This shows the equivalence of the two definitions.

There is also an alternate definition of the period. Choose any $x \in X(\overline{K})$. The cocycle $\sigma \mapsto {}^\sigma x - x$ furnishes a cohomology class in $\xi \in \mathrm{H}^1(K, J)$, where $J$ is the Jacobian variety of $X$. Let $\operatorname{Pic}^1_{X/K}$ be the connected component of the Picard scheme of $X$ representing degree 1 invertible sheaves; it is a principal homogeneous space for $J = \operatorname{Pic}^0_{X/K}$. As such, there is a class in $\mathrm{H}^1(K, J)$ representing $\operatorname{Pic}^1_{X/K}$, and in fact one sees that this class is $\xi$. Similarly, $n\xi$ represents $\operatorname{Pic}^n_{X/K}$. We know that $\operatorname{Pic}^n_{X/K}$ is a trivial principal homogeneous space for $J$ precisely when it possesses a $K$-point. Such a point occurs when there is a Galois-invariant element of $\operatorname{Pic}^n \overline{X}$. Thus we may define the period as the order of $\xi$.

Note that when $X$ is a genus one curve, $X$ itself equals $\operatorname{Pic}^1_{X/K}$, and $\xi$ represents $X$ as an element of $\mathrm{H}^1(K, E)$, where $E$ is the Jacobian of $X$. We say a field $L$ *splits*

$X$ if $X(L) \neq \emptyset$. For $X$ a genus 1 curve represented by $\xi \in \mathrm{H}^1(K,E)$, $L$ splits $X$ if and only if $\xi$ lies in the kernel of the restriction map $\mathrm{H}^1(K,E) \to \mathrm{H}^1(L,E)$.

We now reduce the proof of Theorem 1.2 to the case where $n$ (and hence $\ell$) is a prime power.

**Lemma 2.1.** *Let $P_1, P_2, I_1$, and $I_2$ be positive integers such that the $P_i$ are relatively prime and $P_i \mid I_i \mid P_i^2$. Let $E$ be an elliptic curve over a field $K$. If there are genus one curves $X_1$ and $X_2$ over $K$ with Jacobian $E$ such that $X_i$ has period $P_i$ and index $I_i$, then there is also a curve $X$ with Jacobian $E$ having period $P_1P_2$ and index $I_1I_2$.*

*Proof.* Let $\xi_i \in \mathrm{H}^1(K,E)$ represent $X_i$. I claim that $\xi := \xi_1 + \xi_2$ has period $P_1P_2$ and index $I_1I_2$.

Since the period is the order of $\xi$ in $\mathrm{H}^1(K,E)$, the first part of the claim is obvious. Now suppose that $\xi$ has index $I$. If $L$ is a finite extension of $K$ which splits $\xi$, then $\xi$ lies in the kernel of the restriction map $\mathrm{res} : \mathrm{H}^1(K,E) \to \mathrm{H}^1(L,E)$. Since the orders of the $\xi_i$ are relatively prime and res is a homomorphism, $L$ splits both of the $\xi_i$ as well. Therefore $I_1I_2$ divides $I$. On the other hand, any field which splits both of the $\xi_i$ splits $\xi$ as well. In particular, we can choose fields of the form $L_1 \cdot L_2$ where each $L_i$ splits $\xi_i$. Varying over all such choices, one sees that $I \mid I_1I_2$. □

2.2. **O'Neil's obstruction map.** Our main tool for computing the index is O'Neil's obstruction map. In order to define it, we first construct a *theta group*. Let $E[n]$ be the $n$-torsion points of the elliptic curve $E$, viewed as a group scheme over $K$. Then our theta group is a central extension $\mathscr{G}(n)$ in the category of group schemes over $K$ given by the exact sequence

$$0 \to \mathbb{G}_m \to \mathscr{G}(n) \to E[n] \to 0, \tag{2.1}$$

where the commutator is given by the Weil pairing. That is, $\mathscr{G}(n)$ as a scheme is just $\mathbb{G}_m \times E[n]$, but with multiplication satisfying

$$(x,S)(y,T)(x,S)^{-1}(y,T)^{-1} = (e_n(S,T), O),$$

where $e_n$ is the Weil pairing on $E[n]$ and $O$ is the identity of $E$; see [14, §23] or [13] for more details. Taking (nonabelian) Galois cohomology, one obtains a map

$$\mathrm{Ob} : \mathrm{H}^1(K, E[n]) \to \mathrm{H}^2(K, \mathbb{G}_m) = \mathrm{Br}\, K.$$

This is the obstruction map. Note that it is a *quadratic* map, not a homomorphism. (Quadratic essentially means that $\mathrm{Ob}(\xi) = b(\xi,\xi)$ for some bilinear map $b$.) This results from the fact that $\mathscr{G}(n)$ is a noncommutative group scheme, and hence our cohomology sequence takes place in nonabelian Galois cohomology; see Zarhin [22].

Recall the Kummer sequence for $E$ gives rise to the exact sequence in Galois cohomology

$$0 \to E(K)/nE(K) \to \mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(K,E)[n] \to 0. \tag{2.2}$$

Thus, if $X$ has period dividing $n$, there exist (usually many) $\xi \in \mathrm{H}^1(K, E[n])$ representing it; that is, the image of $\xi$ in $\mathrm{H}^1(K,E)[n]$ represents $X$ in the usual sense.

In [15], O'Neil showed

**Proposition 2.2.** *The image of the obstruction map lies in* $(\mathrm{Br}\, K)[n]$*. If* $\mathrm{Ob}(\xi)$ *has order* $\ell$*, then the index of the curve* $X$ *represented by* $\xi$ *divides* $n\ell$*. If* $X$ *has index* $n$*, then there is a class* $\xi$ *representing* $X$ *such that* $\mathrm{Ob}(\xi) = 0$*.*

The idea is that $\mathrm{H}^1(K, E[n])$ classifies principal homogeneous spaces $X$ for $E$ over $K$ *along with* a choice of Galois-invariant degree $n$ invertible sheaf $\mathscr{L} \in (\mathrm{Pic}\, \overline{X})^G$, up to isomorphism over $K$. Specifically, any cocycle in the class of $\xi$ gives rise to a $\overline{K}$-isomorphism $\varphi : E \to X$. Then $\mathscr{L} = \mathscr{L}(n\varphi(O))$. One sees that $\Gamma(\overline{X}, \mathscr{L})/\overline{K}^\times$ forms a twist of $\mathbb{P}^{n-1}$ over $K$—that is, a Brauer-Severi variety. The obstruction map takes the pair $(X, \mathscr{L})$ to the class of this Brauer-Severi variety in $\mathrm{Br}\, K$. From this characterization, the proposition is easy: If $X$ has index $n$, then there is a rational divisor $D$ of degree $n$. The class $\xi$ representing $(X, \mathscr{L}(D))$ satisfies $\mathrm{Ob}(\xi) = 0$. If $\mathrm{Ob}(\xi)$ has order $\ell$ and $\xi$ represents the pair $(X, \mathscr{L})$, then the Brauer-Severi variety arising from $\mathscr{L}$ is split by an extension of degree $\ell$. Then the tensor product $\mathscr{L}^\ell$ is a class of degree $n\ell$ containing a rational divisor. See [15] for more details.

One would hope that the converse held: if $X$ has index $n\ell$, then there ought to be $\xi$ representing $X$ such that $\mathrm{Ob}(\xi)$ has order $\ell$. However, this is not known to be true. We will use a trick in proving the main theorem to construct $X$ for which this does hold.

Let $\delta$ be the composition $E(K) \to E(K)/nE(K) \to \mathrm{H}^1(K, E[n])$, where the latter map is given by the map in (2.2). For $x \in E(K)$ and $X$ a principal homogeneous space for $E$ over $K$, let $T(x, X)$ denote the Tate pairing of $X$ with the image of $x$ in $E(K)/nE(K)$. Then

**Proposition 2.3.** $\mathrm{Ob}(\xi + \delta x) = \mathrm{Ob}(\xi) + T(x, X)$*.*

*Proof.* See [15, §5]. □

O'Neil's introduction of the obstruction map is useful because in many cases it may be computed using a Hilbert symbol, which we now define. Let $K$ be a field of characteristic not dividing $n$ which contains $\mu_n$, the $n$th roots of unity. Let $a, b \in K^\times/K^{\times n}$. By Kummer theory, we know that $K^\times/K^{\times n} = \mathrm{H}^1(K, \mu_n)$. The cup product gives a map

$$K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mathrm{H}^2(K, \mu_n \otimes \mu_n).$$

Fix a primitive $n$th root of unity $\zeta$. Define an isomorphism $\mu_n \otimes \mu_n \to \mu_n$ by $\zeta^i \otimes \zeta^j \mapsto \zeta^{ij}$, which induces an isomorphism $\mathrm{H}^2(K, \mu_n \otimes \mu_n) \to \mathrm{H}^2(K, \mu_n)$. Using the fact that $\mathrm{H}^2(K, \mu_n) = (\mathrm{Br}\, K)[n]$, we see that the composition gives a pairing

$$\begin{aligned} K^\times/K^{\times n} \times K^\times/K^{\times n} &\to (\mathrm{Br}\, K)[n] \\ (a, b) &\mapsto \langle a, b \rangle \end{aligned}$$

which we call the Hilbert symbol. If we let $w = (a, b)$, then we will alternatively write $\langle w \rangle$ for $\langle a, b \rangle$. Since the cup product is bilinear and skew-symmetric, so is the Hilbert symbol.

Note that the Hilbert symbol depends on $n$ and $\zeta$. Frequently we will abuse notation and define the Hilbert symbol as a map $(K^\times)^2 \to \mathrm{Br}\, K$, by composing with the obvious quotient map.

We return to the obstruction map. Assume that the $n$-torsion of $E$ is rational over $K$. By the theory of the Weil pairing, $\mu_n \subset K$. Let $\zeta$ be the previously chosen primitive $n$th root of unity. Fix a basis $(S, T)$ for $E[n]$ such that $e(S, T) = \zeta$, where $e$ is the Weil pairing.. The choice of basis, and our fixed generator $\zeta$ of $\mu_n$,

yields an isomorphism of (trivial) Galois-modules $E[n] \cong \mu_n \times \mu_n$, and we have an isomorphism

$$\kappa : \mathrm{H}^1(K, E[n]) \to K^\times/K^{\times n} \times K^\times/K^{\times n}.$$

**Proposition 2.4.** *Let $\xi \in \mathrm{H}^1(K, E[n])$. If $n$ is odd or $E[2n] \subset E(K)$, then $\mathrm{Ob}(\xi) = \langle \kappa(\xi) \rangle$. If $n$ is even, then $2\,\mathrm{Ob}(\xi) = 2\langle \kappa(\xi) \rangle$.*

*Proof.* For the case that $n$ is odd, see [15, Prop. 3.4] and [16]. A proof in the even case, including an explicit computation of $\mathrm{Ob}(\xi) - \langle \kappa(\xi) \rangle$, can be found in [4, §2]. □

Assume from now on that $K$ is a number field. If $v$ is a place of $K$, write $K_v$ for the completion of $K$ at $v$. In order to use the Hilbert symbol, we will reduce to the local case using the fact that, if $K$ is a global field, $\mathrm{Br}\, K = \oplus_v \mathrm{Br}\, K_v$. That is, in order to compute $\langle a, b \rangle$, it suffices to compute $\langle a, b \rangle_v$, where the latter symbol is computed in $K_v$, and $a, b$ are considered as elements of $K_v$.

(More generally, for any $K$-group scheme $M$ and integer $q$, we have a natural localization map

$$\mathrm{H}^q(K, M) \to \mathrm{H}^q(K_v, M)$$

in étale cohomology. We will denote this map by adding the subscript $v$; e.g. $\xi \mapsto \xi_v$.)

If $v$ is a place of $K$, we also use $v$ to denote a fixed corresponding valuation.

**Lemma 2.5.** *Let $K_v$ be a nonarchimedean local field such that $v(n) = 0$. Let $\pi$ be a uniformizing parameter and $u, u'$ units; that is, $v(u) = v(u') = 0$. Let $\mathbb{F}$ be the residue field of $K_v$.*

(1) $\langle u, u' \rangle_v = 0$.
(2) *The order of $\langle u, \pi \rangle_v$ equals the order of the image of $u$ in $\mathbb{F}^\times/\mathbb{F}^{\times n}$.*

*Proof.* According to [17, Ch. XIV], $\langle a, b \rangle_v = 0$ if and only if $b$ is a norm from the extension $K_v(a^{1/n})/K_v$. The extension $K_v(u^{1/n})$ is unramified with degree, say, $d$, which by Hensel's Lemma also equals the order of $u$ in $\mathbb{F}^\times/\mathbb{F}^{\times n}$. According to local class field theory, the norm from an unramified extension of degree $d$ is precisely the set of elements $x$ such that $v(x)$ is a multiple of $dv(\pi)$. The result follows immediately for the first claim, and from bilinearity for the second claim. □

We also have the following:

**Proposition 2.6.** *For $a, b \in K^\times$, $\displaystyle\sum_v \langle a, b \rangle_v = 0$.*

Here, we use the fact that $\mathrm{Br}\, K_v$ is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$, $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, or 0 via the *invariant map* so that the sum makes sense. For the remainder of this paper, we identify $\mathrm{Br}\, K_v$ with the appropriate subgroup of $\mathbb{Q}/\mathbb{Z}$. Note that the sum is finite: there are finitely many archimedean primes, and for all but finitely many nonarchimedean $v$, $v(a) = v(b) = v(n) = 0$, so that by Lemma 2.5, $\langle a, b \rangle_v = 0$.

*Proof.* This follows from the fact that $\mathrm{Br}\, K$ is isomorphic to the set of $(t_v)$, $t_v \in \mathrm{Br}\, K_v$, such that almost all $t_v = 0$ and $\sum t_v = 0$; and the fact that cup products, and hence the Hilbert symbol, commute with localization. □

In order to deal with the fact that the obstruction map does not necessarily give a sharp bound on index, we will use obstruction maps of different levels. We define $\mathrm{Ob}_n$ to be the corresponding obstruction map $\mathrm{H}^1(K, E[n]) \to \mathrm{Br}\, K$.

**Proposition 2.7.** *Let $n$ and $m$ be positive integers. The following diagrams commute:*

(1)

$$\begin{tikzcd} \mathrm{H}^1(K, E[n]) \arrow[r, "\mathrm{Ob}_n"] \arrow[d, "j_*"'] & \operatorname{Br} K \arrow[d, "m"] \\ \mathrm{H}^1(K, E[mn]) \arrow[r, "\mathrm{Ob}_{mn}"] & \operatorname{Br} K \end{tikzcd}$$

*where $j_*$ is induced by the canonical inclusion $j : E[n] \to E[mn]$, and $m$ is muliplication by $m$.*

(2)

$$\begin{tikzcd} \mathrm{H}^1(K, E[mn]) \arrow[r, "\mathrm{Ob}_{mn}"] \arrow[d, "{[m]}"'] & \operatorname{Br} K \arrow[d, "m"] \\ \mathrm{H}^1(K, E[n]) \arrow[r, "\mathrm{Ob}_n"] & \operatorname{Br} K \end{tikzcd}$$

*where $[m]$ is the map induced by the multiplication by $m$ map $E[mn] \to E[n]$.*

(3)

$$\begin{tikzcd} \mathrm{H}^1(K, E[n]) \arrow[r, "\mathrm{Ob}_n"] \arrow[d, "\mathrm{res}"'] & \operatorname{Br} K \arrow[d, "\mathrm{res}"] \\ \mathrm{H}^1(L, E[n]) \arrow[r, "\mathrm{Ob}_n"] & \operatorname{Br} L \end{tikzcd}$$

*where $L/K$ is a field extension and* res *is the restriction map.*

*Proof.* Let $\xi \in \mathrm{H}^1(K, E[n])$ represent the pair $(X, \mathscr{L})$, where $\mathscr{L}$ is the divisor class of $n(x)$ for some $x \in X(\overline{K})$. Then $j_*(\xi)$ represents $(X, \mathscr{L}^m)$. The map which takes elements of $(\operatorname{Pic} \overline{X})^G$ to the class of the associated Brauer-Severi variety is a homomorphism; indeed, it arises from the Leray spectral sequence $\mathrm{H}^p(K, \mathrm{H}^q(\overline{X}, \mathbb{G}_m)) \Rightarrow \mathrm{H}^{p+q}(X, \mathbb{G}_m)$, which yields the exact sequence

$$0 \to \operatorname{Pic} X \to \mathrm{H}^0(K, \operatorname{Pic} \overline{X}) \to \mathrm{H}^2(K, \mathbb{G}_m).$$

The last map sends an invertible sheaf to the class of its associated Brauer-Severi variety; see for example [9]. The first part of the proposition follows.

For the second part, Mumford showed [13, p. 309–310] that multiplication by $m$ extends to a homomorphism on theta groups $\mathscr{G}(mn) \to \mathscr{G}(n)$. The restriction of this homomorphism to $\mathbb{G}_m$ is also multiplication by $m$. Taking the long cohomology sequence associated to (2.1), we obtain the commutative diagram.

The third part is obvious, since $\operatorname{res} \xi$ represents the same pair $(X, \mathscr{L})$ as $\xi$ does, but over $L$. □

Similar to $\mathrm{Ob}_n$, we define $\delta_n$ to be the composition $E(K) \to E(K)/nE(K) \to \mathrm{H}^1(K, E[n])$, where the second map in the composition is the coboundary coming from the Kummer sequence for $E$.

## 3. The case of rational torsion

By Lemma 2.1, we may assume that $n$ is a prime power $p^r$; this assumption holds for the remainder of the paper. In this section, we will prove the theorem under the additional assumption that $E[n] \subset E(K)$ in the case that $p$ is odd, and $E[2n] \subset E(K)$ if $p = 2$.

3.1. **Choosing a pair of primes.** Our first step is to find a pair of distinct nonarchimedean primes $v$, $v'$ satisfying certain splitting conditions. (We use primes and places interchangeably.) We state the conditions below, after which we show that infinitely many pairs $v$, $v'$ satisfying the conditions exist. The proof is essentially repeated use of the Cebotarev density theorem. Let $S$ be the union of the primes $w$ of $K$ such that $E$ has bad reduction at $w$, archimedean primes, and primes dividing $n$. The conditions are

- A1. The primes $v$,$v'$ are principal with totally positive generators $\pi$ and $\pi'$ respectively.
- A2. Let $E(K)$ embed in $E(K_v)$ in the usual manner. Then $E(K)$ lies in $nE(K_v)$.
- A3. For each $w \in S$, $\pi$ and $\pi'$ lie in $K_w^{\times n}$.
- A4. The order of the image of $\pi'$ in $K_v^\times / K_v^{\times n}$ is exactly $n$.

**Lemma 3.1.** *There exist infinitely many pairs of distinct primes $v$, $v'$ satisfying conditions A1–A4.*

*Proof.* Condition A1 is equivalent to $v$ and $v'$ splitting completely in the Hilbert class field of $K$.

Condition A2 is the same as requiring $v$ to split completely in $K([n]^{-1}E(K))$; that is, the field obtained by adjoining to $K$ all $x \in E(\overline{K})$ such that $[n]x \in E(K)$. By [19, p.194], $K([n]^{-1}E(K))$ is a finite abelian extension which is unramified outside $S$.

Let $\mathfrak{m}$ be the modulus given by the product of $n^2$ and all primes where $E$ has bad reduction. Let $K_{\mathfrak{m}}$ be the ray class field for $K$ with modulus $\mathfrak{m}$. Then condition A3 holds if $v$ and $v'$ split completely in $K_{\mathfrak{m}}$; for in that case, the Frobenius for $v$ (say) is trivial and, by class field theory, $v$ has a generator $\pi$ which is congruent to $1 \pmod{\mathfrak{m}}$. Then Hensel's Lemma implies A3.

We now choose $v$ to be any prime which splits completely in the compositum of the three fields named above. Next we tackle A4.

By abuse of notation, let $v$ be a valuation corresponding to the prime $v$. Let $\alpha \in K$ be any element such that $v(\alpha) = 0$ and whose image in $K_v^\times / K_v^{\times n}$ has order $n$; since $\pi \cong 1 \pmod{\mathfrak{m}}$, and $n \mid \mathfrak{m}$, there exists such $\alpha$ in $K_v$. But $K$ is dense in $K_v$, so we may find such $\alpha$ in $K$. Let $F'$ be the ray class field with modulus $v$. By class field theory, the Galois group $\mathrm{Gal}(F'/K)$ is isomorphic to the class group with modulus $v$. In particular, if $v'$ and $(\alpha)$ lie in the same class in this class group, then $v'$ has a generator $\pi'$ which is congruent to $\alpha \pmod{v}$, and hence satisfies A4.

Let $F$ be the compositum of $K_{\mathfrak{m}}$ and $K([n]^{-1}E(K))$. We see that $F'$ is unramified outside $v$, while $F$ is unramified at $v$. Hence $F \cap F'$ lies in the Hilbert class field of $K$. To satisfy A1–A3, we wish $v'$ to split completely in $F$, while to satisfy A4, we wish $v'$ to lie in the class of $(\alpha)$ in the appropriate ray class group. These conditions are compatible since they both imply that $v'$ splits completely in the Hilbert class field of $K$. Thus we may apply the Cebotarev density theorem to find infinitely many such $v'$ and $\pi'$. $\square$

3.2. **Construction of curve.** As mentioned earlier, a choice of ordered basis $(S,T)$ for $E[n]$ with $e(S,T)=\zeta$ yields an isomorphism

$$\kappa : \mathrm{H}^1(K,E[n]) \to K^\times/K^{\times n} \times K^\times/K^{\times n}.$$

Choose $\xi \in \mathrm{H}^1(K,E[n])$ such that $\kappa(\xi) = (\pi, \pi'^{n/\ell})$. Let $X$ be the corresponding principal homogeneous space for $E$.

**Proposition 3.2.** *The curve $X$ has period $n$ and index $n\ell$.*

*Proof.* For any positive integer $m$, we have $\kappa(m\xi) = (\pi^m, \pi'^{mn/\ell})$. Let $v$ be the place of $K$ lying over $(\pi)$, and suppose $m < n$. If the curve associated to $m\xi$ is a trivial principal homogeneous space, then there exists $x \in E(K)$ such that $\kappa(\delta x + m\xi) = (1,1)$, where we recall that $\delta$ is the composition

$$E(K) \to E(K)/nE(K) \to \mathrm{H}^1(K,E[n]).$$

But by condition A2, $x$ lies in $nE(K_v)$. Hence $(\delta x)_v = 0$. Therefore for any choice of $x$, $\kappa(\delta x + m\xi)_v = (\pi^m, \cdot\,)$, and so $m\xi$ yields a trivial principal homogeneous space if and only if $n \mid m$. Therefore the period of $X$ is $n$.

By Proposition 2.4, $\mathrm{Ob}(\xi) = \langle \pi, \pi'^{n/\ell}\rangle$. We compute the Hilbert symbol locally. For places $w$ satisfying $w(n) > 0$, condition A3 shows that

$$\langle \pi, \pi'^{n/\ell}\rangle_w = 0.$$

Let $v'$ be the place corresponding to $\pi'$. For $w \neq v, v'$ and $w(n) = 0$, $\pi$ and $\pi'$ are both units in $K_w$, and so by Lemma 2.5 the local Hilbert symbol is zero. By Proposition 2.6, the order of the Hilbert symbol at $v$ equals that at $v'$, so we need only consider $v$. Combining condition A4 with Lemma 2.5, we see that $\langle \pi, \pi'^{n/\ell}\rangle$ has order $\ell$. Hence $\mathrm{Ob}(\xi)$ has order $\ell$, and the index of $X$ divides $n\ell$.

Let $\ell'$ strictly divide $\ell$, and let $j_*$ be the canonical map

$$\mathrm{H}^1(K,E[n]) \to \mathrm{H}^1(K,E[n\ell']).$$

If $X$ had index $n\ell'$, then by Lemma 2.2 there would exist $x$ in $E(K)$ such that

$$\mathrm{Ob}_{n\ell'}(\delta_{n\ell'} x + j_*(\xi)) = 0.$$

According to Proposition 2.3, the above equals

$$\mathrm{Ob}_{n\ell'}(j_*(\xi)) + T(x,X).$$

By condition A2, $x \in nE(K_v)$ and hence $T(x,X)_v = 0$. But by Proposition 2.7, $\mathrm{Ob}_{n\ell'} j_*(\xi) = \ell' \,\mathrm{Ob}_n \xi \neq 0$ if $\ell' < \ell$. Therefore the index of $X$ is precisely $n\ell$. $\square$

## 4. Proof of Main Theorem, odd $n$

For now, we assume $n$ is odd. We suppose either: a) $\mu_n \subset K$, or b) $E$ contains a Galois-stable subgroup of order $n$. Over $L := K(E[n])$, we may use the arguments of the previous section to construct a cohomology class $\xi \in \mathrm{H}^1(L,E[n])$ with the desired properties. Let cores be the corestriction map

$$\mathrm{cores} : \mathrm{H}^1(L,E[n]) \to \mathrm{H}^1(K,E[n]).$$

We will show that $\mathrm{cores}\,\xi$ represents a curve over $K$ with period $n$ and index $n\ell$. In order to compute the index, we will need to base extend back to $L$; in other words, we'll compute $\mathrm{res} \circ \mathrm{cores}\,\xi$, where res is the restriction map

$$\mathrm{res} : \mathrm{H}^1(K,E[n]) \to \mathrm{H}^1(L,E[n]).$$

4.1. **Pairs of primes.** As in the previous section, we wish to choose principal primes of $L$, $(\pi)$ and $(\pi')$, such that analogues to conditions A1–A4 hold, along with a new condition. For any place $w$ of $L$, let $w_K$ denote the place of $K$ lying below $w$. Let $S$ be the set of primes $w$ of $L$ such that $E$ has bad reduction at $w_K$, $w_K$ is archimedean, or $w_K(n) > 0$.

We now state the relevant conditions.

- B1. The primes $v = (\pi)$ and $v' = (\pi')$ are principal, with totally positive generators $\pi$ and $\pi'$.
- B2. Under the usual embedding, $E(K)$ lies in $nE(K_{v_K})$.
- B3. The generators $\pi$ and $\pi'$ lie in $L_w^{\times n}$ for all $w \in S$.
- B4. The order of the image of $\pi'$ in $L_v^\times / L_v^{\times n}$ is $n$. Additionally, $\sigma\pi'$ lies in $L_v^{\times n}$ for all nontrivial $\sigma \in \mathrm{Gal}(L/K)$.
- B5. The primes $v_K, v'_K$ split completely in $L$.

**Lemma 4.1.** *There are infinitely many pairs of primes $(\pi)$, $(\pi')$ satisfying conditions B1–B5.*

*Proof.* Let $\mathfrak{m}$ be the modulus over $L$ given as the product of $n^2$ and all primes $w$ in $S$. Let $L_\mathfrak{m}$ be the ray class field of $L$ with modulus $\mathfrak{m}$. The modulus $\mathfrak{m}$ is rational over $K$, so that $L_\mathfrak{m}$ is Galois over $K$. Let $F$ be the compositum of $L_\mathfrak{m}$, $K([n]^{-1}E(K))$, and the Hilbert class field of $K$. By the Cebotarev density theorem, there exists infinitely many primes $v_K$ of $K$ which split completely in $F$. Setting $v$ equal to any prime of $L$ lying over $v_K$, we use the same reasoning as in Lemma 3.1 to see that $v$ satisfies conditions B1–B5.

Choose any unit $\beta$ in $L_v$ which has order $n$ in $L_v^\times / L_v^{\times n}$. By the Chinese Remainder Theorem, there exists $\alpha \in L$ such that

$$\begin{aligned} &\alpha \equiv \beta \pmod{v} \\ &\alpha \equiv 1 \pmod{\sigma v} \quad \forall \sigma \neq 1 \in \mathrm{Gal}(L/K) \end{aligned} \tag{4.1}$$

Let $F'$ be the ray class field for $L$ with modulus $\prod \sigma v$. The modulus is rational over $K$, so that $F'$ is Galois over $K$. The Galois group $\mathrm{Gal}(F'/L)$ is isomorphic to the class group with modulus $\prod \sigma v$ via the Artin reciprocity map. Let $\gamma_L$ in $\mathrm{Gal}(F'/L)$ map to the class of $(\alpha)$ under this isomorphism. Then under the inclusion $\mathrm{Gal}(F'/L) \hookrightarrow \mathrm{Gal}(F'/K)$, $\gamma_L$ maps to, say, $\gamma$. Let $[\gamma]$ be the conjugacy class of $\gamma$ in $\mathrm{Gal}(F'/K)$.

One can find $\tau \in \mathrm{Gal}(F'F/K)$ such that $\tau|_{F'}$ lies in $[\gamma]$, and $\tau|_F$ is trivial. This follows because $F'/L$ is ramified only at the $\sigma v$, while $F/L$ is unramified at those places; therefore $F \cap F'$ is contained in the Hilbert class field of $L$. But $\gamma$ acts trivially on the Hilbert class field since $(\alpha)$ is principal. Therefore, $\tau$ as prescribed exists.

Now we apply the Cebotarev density theorem again to find $v'_K$ corresponding to the conjugacy class of $\tau$. Choosing $v'$ to be any place of $L$ lying over $v'_K$, we use the same reasoning as before to conclude that $v'$ satisfies the conditions. □

4.2. **The corestriction map.** As before, choose a basis $(S, T)$ for $E[n]$ such that $e(S, T) = \zeta$. If we are under the hypothesis that $E$ contains a Galois-stable order $n$ subgroup, choose our basis so that $S$ generates this subgroup. As before, our choice of basis yields an isomorphism

$$\kappa : \mathrm{H}^1(L, E[n]) \to L^\times / L^{\times n} \times L^\times / L^{\times n}$$

Let $\pi, \pi'$ be as in the previous section, and choose $\xi$ so that $\kappa(\xi) = (\pi, \pi')$. Let $\mathrm{cores} : \mathrm{H}^1(L, E[n]) \to \mathrm{H}^1(K, E[n])$ be the corestriction map, and $\eta = \mathrm{cores}(\xi)$. We wish to show that the curve corresponding to $\eta$ satisfies the conditions of our theorem. But it is too difficult to compute the obstruction map $\mathrm{Ob}(\eta)$, so we will instead use $\mathrm{Ob}(\mathrm{res}\,\eta)$, where res is the restriction map

$$\mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(L, E[n]).$$

Therefore, we need to compute $\mathrm{res} \circ \mathrm{cores}(\xi)$. Note that $\mathrm{cores} \circ \mathrm{res}$ is well-known and equal to $[L : K]$, but the same is not true of $\mathrm{res} \circ \mathrm{cores}$.

For any $G_K$-module $M$ and nonnegative integer $r$, one has an action of $\mathrm{Gal}(L/K)$ on $\mathrm{H}^r(L, M)$. This action is induced by the action on homogeneous $r$-cochains

$$c^\sigma(\gamma_1, \ldots, \gamma_r) = \sigma c(\sigma^{-1}\gamma_1\sigma, \ldots, \sigma^{-1}\gamma_r\sigma)$$

where $\sigma \in \mathrm{Gal}(L/K)$ and $\gamma_i \in G_L$. (Actually, we must lift $\sigma$ to any fixed element of $G_K$ when acting by conjugation on the $\gamma_i$.) Define $\mathrm{Nm} : \mathrm{H}^r(L, M) \to \mathrm{H}^r(L, M)$ by

$$\mathrm{Nm}(\theta) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \theta^\sigma.$$

**Lemma 4.2.** *For $\theta \in \mathrm{H}^r(L, M)$,* $\mathrm{res} \circ \mathrm{cores}\,\theta = \mathrm{Nm}\,\theta$*, where* res *and* cores *are the obvious restriction and corestriction maps.*

*Proof.* This follows from the definition of corestriction and dimension shifting; see [17, p. 119]. □

Therefore $\mathrm{cores}\,\eta = \mathrm{Nm}\,\xi$. Unfortunately, $\kappa$ is not $\mathrm{Gal}(L/K)$-equivariant, so that $\kappa(\mathrm{Nm}\,\xi) \neq (\mathrm{Nm}\,\pi, \mathrm{Nm}\,\pi')$. Instead, we have a *twisted* norm on $L^\times/L^{\times n} \times L^\times/L^{\times n}$, which we now describe. Let

$$\begin{aligned} \mathrm{Gal}(L/K) &\to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ \sigma &\mapsto M_\sigma \end{aligned}$$

be the representation of $\mathrm{Gal}(L/K)$ on $E[n]$ with respect to the basis $(S, T)$. The determinant of $M_\sigma$ is given by the $n$th cyclotomic character. If $\mu_n \subset K$, then the determinant is identically 1, and hence the representation lies in $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. If $S$ generates a Galois-stable subgroup, then the representation lies in the set of upper-triangular matrices.

**Proposition 4.3.** *Suppose $\sigma \in \mathrm{Gal}(L/K)$, $\xi \in \mathrm{H}^1(L, E[n])$ and $\kappa(\xi) = (a, b)$. Then*

$$\kappa(\xi^\sigma) = \frac{M_\sigma}{\det M_\sigma}(\sigma a, \sigma b)$$

*where for $M \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, if*

$$M = \begin{bmatrix} i & j \\ k & l \end{bmatrix},$$

*then $M(a, b) = (a^i b^j, a^k b^l)$.*

*Proof.* Let $\rho : E[n] \to \mu_n \times \mu_n$ be the isomorphism given by the basis $(S, T)$. Write $(\mu_n \times \mu_n)_\rho$ for the $\mathrm{Gal}(L/K)$-module with underlying group $\mu_n \times \mu_n$, but with

module-structure making $\rho$ an isomorphism of Galois modules; that is

$$\begin{aligned}\sigma(\zeta_1,\zeta_2)_\rho &= \rho\sigma\rho^{-1}(\zeta_1,\zeta_2)\\ &= M_\sigma(\zeta_1,\zeta_2).\end{aligned}$$

Consider the diagram

$$\begin{tikzcd} L^\times/L^{\times n}\times L^\times/L^{\times n} \arrow[r, "\psi"] & \mathrm{H}^1(L,\mu_n\times\mu_n) \arrow[d, "i_*"] & \\ & \mathrm{H}^1(L,(\mu_n\times\mu_n)_\rho) \arrow[r, "\varphi"'] & \mathrm{H}^1(L,E[n]) \end{tikzcd} \tag{4.2}$$

The isomorphism $\psi$ comes from the usual Kummer isomorphism. The map $i_*$ is induced by the canonical isomorphism of the underlying groups $i:\mu_n\times\mu_n\to(\mu_n\times\mu_n)_\rho$. The map $\varphi$ is induced by the map sending $(\zeta,1)$ to $S$ and $(1,\zeta)$ to $T$ (compare to $\kappa^{-1}$). Then the horizontal arrows are both $\mathrm{Gal}(L/K)$-equivariant, and the composition $\varphi i_*\psi$ is equal to $\kappa^{-1}$.

Let $\gamma\in\mathrm{Gal}(\overline{L}/L)$ and lift $\sigma$ arbitrarily to an element, also written $\sigma$, of $\mathrm{Gal}(\overline{K}/K)$. We have

$$[i_*\psi(a,b)]^\sigma(\gamma) = \sigma i(\psi(a,b)(\sigma^{-1}\gamma\sigma)) \tag{4.3}$$
$$= \sigma i(\sigma^{-1}\sigma\psi(a,b)(\sigma^{-1}\gamma\sigma)) \tag{4.4}$$
$$= \sigma i(\sigma^{-1}\psi(a,b)^\sigma(\gamma)) \tag{4.5}$$
$$= \sigma i(\sigma^{-1}[\psi(\sigma a,\sigma b)(\gamma)]) \tag{4.6}$$
$$= \frac{M_\sigma}{\det M_\sigma} i[\psi(\sigma a,\sigma b)(\gamma)] \tag{4.7}$$
$$= i_*\psi\left(\frac{M_\sigma}{\det M_\sigma}(\sigma a,\sigma b)\right)(\gamma). \tag{4.8}$$

The equality (4.5) follows by the definition of the $\mathrm{Gal}(L/K)$-action on $\mathrm{H}^1(L,\mu_n\times\mu_n)$. Since $\psi$ is a $\mathrm{Gal}(L/K)$-morphism, we obtain (4.6). Finally, (4.7) follows from the action of $\sigma$ on $E[n]$ by the matrix $M_\sigma$, and the action of $\sigma^{-1}$ on $\mu_n\times\mu_n$ by $(\det M_\sigma)^{-1}$.

Now apply $\varphi$ to both sides of the equation to obtain

$$[\kappa^{-1}(a,b)]^\sigma = \kappa^{-1}\left(\frac{M_\sigma}{\det M_\sigma}(\sigma a,\sigma b)\right)$$

from which the lemma follows. □

**Corollary 4.4.** *Let $\kappa(\xi)=(a,b)$. Then $\kappa(\mathrm{Nm}\,\xi)$ equals*

$$\left(\prod(\det M_\sigma)^{-1}\sigma a^{i(\sigma)}\sigma b^{j(\sigma)},\ \prod(\det M_\sigma)^{-1}\sigma a^{k(\sigma)}\sigma b^{\ell(\sigma)}\right)$$

*where the product is taken over $\sigma\in\mathrm{Gal}(L/K)$.*

4.3. **Computation of the obstruction map.** Let $\xi\in\mathrm{H}^1(L,E[n])$ satisfy $\kappa(\xi)=(\pi,\pi'^{n/\ell})$, where $\pi$ and $\pi'$ were chosen as in Lemma 4.1. Let $\eta=\mathrm{cores}\,\xi$. In order to compute $\mathrm{Ob}(\eta)$, we instead compute $\mathrm{res}\,\mathrm{Ob}(\eta)=\mathrm{Ob}(\mathrm{res}\,\eta)$, or $\mathrm{Ob}(\mathrm{Nm}\,\xi)$. But

the $n$-torsion $E[n]$ is rational over $L$, so by Proposition 2.4 we may use the Hilbert symbol to compute $\mathrm{Ob}(\mathrm{Nm}\,\xi)$. Let

$$\begin{aligned} c &= \prod (\det M_\sigma)^{-1} \sigma\pi^{i(\sigma)} \\ d &= \prod (\det M_\sigma)^{-1} \sigma\pi^{k(\sigma)} \\ c' &= \prod (\det M_\sigma)^{-1} \sigma\pi'^{\frac{n}{\ell} j(\sigma)} \\ d' &= \prod (\det M_\sigma)^{-1} \sigma\pi'^{\frac{n}{\ell} l(\sigma)}. \end{aligned}$$

Thus, $\mathrm{Nm}\,\kappa^{-1}(\pi, 1) = \kappa^{-1}(c, d)$, $\mathrm{Nm}\,\kappa^{-1}(1, \pi'^{n/\ell}) = \kappa^{-1}(c', d')$, and $\kappa(\mathrm{Nm}\,\xi) = (cc', dd')$. We wish to compute the Hilbert symbol $\langle cc', dd'\rangle$.

**Lemma 4.5.** *Let $w$ be any place of $L$ satisfying $w(\pi\pi') = 0$. Then the local Hilbert symbol $\langle cc', dd'\rangle_w$ is trivial*

*Proof.* If $w$ is non-archimedean and $w(n) = 0$, then $cc'$ and $dd'$ are both units in $L_w$. Therefore by Lemma 2.5 the Hilbert symbol is trivial.

If $w(n) \neq 0$, then $w$ lies in $S$. According to condition B3, $\pi$, $\pi'$ and their conjugates lie in $L_w^{\times n}$. Again, the Hilbert symbol is trivial.

Lastly, since $n$ is an odd prime power and $\mu_n \subset L$, $L$ has no real embeddings. Therefore the Hilbert symbol at all the archimedean places is automatically trivial. □

**Lemma 4.6.** *Let $v$ be the place of $L$ corresponding to $\pi$. Then $\langle cc', dd'\rangle_v$ has exact order $\ell$.*

*Proof.* By bilinearity, we have

$$\langle cc', dd'\rangle = \langle c, d\rangle + \langle c, d'\rangle + \langle c', d\rangle + \langle d, d'\rangle.$$

Since $c', d, d'$ are all units in $L_v^\times$, the last two terms are zero by Lemma 2.5. Now $c = u\pi$, where $u$ is some unit in $L_v^\times$, so that $\langle c, d'\rangle_v = \langle \pi, d'\rangle_v$. By condition B4, $d' \equiv \pi'^{n/\ell} \pmod{L^{\times n}}$, so that $\langle c, d'\rangle_v = \langle \pi, \pi'^{n/\ell}\rangle_v$. Again applying condition B4 and Lemma 2.5, we see that $\langle c, d'\rangle_v$ has order $\ell$.

We now show that $\langle c, d\rangle_v = 0$. One sees that it suffices to show that $\langle \pi, d\rangle_v = 0$.

Recall that $(S, T)$ was our chosen basis for $E[n]$. If the subgroup generated by $S$ is Galois-stable over $K$, then the $M_\sigma$ are all upper triangular. In particular, $k(\sigma) = 0$ for all $\sigma \in \mathrm{Gal}(L/K)$, which implies that $d = 1$. Therefore $\langle \pi, d\rangle_v = 0$.

Let us assume instead that $\mu_n \subset K$. This immediately implies that $\det M_\sigma = 1$. Since $n$ is odd, it suffices to show that $2\langle \pi, d\rangle_v = 0$. By expanding out $d$ and using bilinearity, we may instead show that

$$\langle \pi, \sigma\pi^{k(\sigma)}\rangle = -\langle \pi, \sigma^{-1}\pi^{k(\sigma^{-1})}\rangle_v.$$

Recall that we write $M_\sigma$ by

$$M_\sigma = \begin{bmatrix} i(\sigma) & j(\sigma) \\ k(\sigma) & l(\sigma) \end{bmatrix}.$$

But $M_{\sigma^{-1}} = M_\sigma^{-1}$. Using $\det M_\sigma = 1$, we obtain

$$M_\sigma^{-1} = \begin{bmatrix} l(\sigma) & -j(\sigma) \\ -k(\sigma) & i(\sigma) \end{bmatrix}.$$

In other words, $k(\sigma^{-1}) = -k(\sigma)$. Therefore it suffices to show that $\langle \pi, \sigma\pi \rangle_v = \langle \pi, \sigma^{-1}\pi \rangle_v$. But we have

$$\begin{aligned} \langle \pi, \sigma\pi \rangle_v &= \langle \sigma^{-1}\pi, \pi \rangle_{\sigma^{-1}v} \\ &= -\langle \pi, \sigma^{-1}\pi \rangle_{\sigma^{-1}v} \\ &= \langle \pi, \sigma^{-1}\pi \rangle_v. \end{aligned}$$

The last equality follows from Proposition 2.6 and the fact that the symbol $\langle \pi, \sigma^{-1}\pi \rangle$ is trivial everywhere but at $v$ and $\sigma^{-1}v$. This proves the lemma. □

Let $v'$ be the place of $L$ corresponding to $\pi'$.

**Proposition 4.7.** $\operatorname{Ob}\eta$ *has order* $\ell$ *at* $v_K$ *and* $v'_K$*, and is trivial at all other places.*

*Proof.* First we prove triviality. For any place $w_K$ of $K$, the corestriction map on $\mathrm{H}^1(L, E[n])$ induces a homomorphism

$$\oplus \operatorname{cores}_w : \oplus \mathrm{H}^1(L_w, E[n]) \to \mathrm{H}^1(K_{w_K}, E[n])$$

where the sum is over all places $w$ of $L$ lying over $w_K$. Recall that $\eta = \operatorname{cores}\xi$. By construction, $\xi$ is locally trivial everywhere except at $v$, $v'$, and their conjugates. Triviality at $w_K \neq v_K, v'_K$ follows.

Since the local invariants of a global Brauer class sum to zero, it suffices to show that $(\operatorname{Ob}\eta)_{v_K}$ has order $\ell$. The diagram

$$\begin{tikzcd} \mathrm{H}^1(K, E[n]) \arrow[r] \arrow[d] & \operatorname{Br} K \arrow[d] \\ \mathrm{H}^1(K_{v_K}, E[n]) \arrow[r] \arrow[d, "\oplus \operatorname{res}"] & \operatorname{Br} K_{v_K} \arrow[d, "\oplus \operatorname{res}"] \\ \oplus \mathrm{H}^1(L_v, E[n]) \arrow[r] & \oplus \operatorname{Br} L_v \end{tikzcd}$$

commutes. The horizontal maps are the relevant obstruction maps. Commutativity follows from functoriality of localization and restriction in nonabelian cohomology. But $v_K$ splits completely in $L$ by condition B5, so that $K_{v_K} \cong L_v$. Thus if we consider the restriction map onto a single factor

$$\begin{tikzcd} \mathrm{H}^1(K_{v_K}, E[n]) \arrow[r] \arrow[d] & \operatorname{Br} K_{v_K} \arrow[d] \\ \mathrm{H}^1(L_v, E[n]) \arrow[r] & \operatorname{Br} L_v \end{tikzcd}$$

then the vertical maps are isomorphism. Therefore the order of $(\operatorname{Ob}\eta)_{v_K}$ equals the order of $(\operatorname{Ob}\operatorname{res}\eta)_v$, or rather $(\operatorname{Ob}\operatorname{Nm}\xi)_v$.

Since $E[n] \subset E(L) \subset E(L_v)$, we may use the Hilbert symbol to evaluate the obstruction map. By construction, $\kappa(\operatorname{Nm}\xi) = (cc', dd')$. The result follows from Lemma 4.6. □

4.4. **End of proof.** Let $X$ be the genus 1 curve over $K$ represented by the class $\eta$ in $\mathrm{H}^1(K, E[n])$. Clearly the period of $X$ divides $n$. Suppose that the period is smaller. Then there is some positive integer $m$ with $m < n$ and some $x \in E(K)$ such that

$$\delta x + m\eta = 0.$$

In particular, this holds locally at $v_K$. But by condition B2, $\delta x$ is trivial at $v_K$ for all $x \in E(K)$. Therefore we must have $m\eta = 0$ at $v_K$. In particular, this must hold when we restrict to $L_v$. But this cannot be, for

$$\begin{aligned}\kappa(\operatorname{res}_{L/K} m\eta) &= m\kappa(\operatorname{res}\eta)\\ &= m(u_1 \cdot \pi, u_2)\\ &= (u_1^m \cdot \pi^m, u_2^m)\end{aligned}$$

for some $u_1$, $u_2$ which are units in $L_v$. We conclude that $X$ has exact period $n$.

By Proposition 4.7, $\operatorname{Ob}\eta$ has order $\ell$. Applying Proposition 2.2, we see that the index of $X$ divides $n\ell$. Suppose the index is $n\ell'$, with $\ell' < \ell$. By Proposition 2.2 there is a class $\eta'$ in $\mathrm{H}^1(K, E[n\ell'])$ representing $X$ such that $\operatorname{Ob}_{n\ell'}\eta' = 0$. Let $j_*$ be the canonical homomorphism

$$\mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(K, E[n\ell']).$$

Since $\eta$ also represents $X$, there exists $x \in E(K)$ such that

$$\eta' = j_*(\eta) + \delta x.$$

By Proposition 2.3,

$$\operatorname{Ob}_{n\ell'}\eta' = \operatorname{Ob}_{n\ell'} j_*(\eta) + T(x, X)$$

where $T$ is the Tate pairing. Consider the latter equation locally at $v_K$. By condition B2, $x$ lies in $nE(K_{v_K})$, so the Tate pairing is zero. The left hand term is zero by hypothesis. But by Proposition 2.7, $\operatorname{Ob}_{n\ell'} j_*(\eta) = \ell' \operatorname{Ob}_n \eta$, and the latter is *not* zero since $\operatorname{Ob}_n \eta$ has order $\ell$ and $\ell' < \ell$. This yields a contradiction. Therefore the index of $X$ must be exactly $n\ell$.

## 5. Even period

Assume now that $n$ is a power of 2. Three problems now arise in the previous arguments.

The first problem is that the obstruction map need not equal the Hilbert symbol; instead, according to Proposition 2.4, $\operatorname{Ob}(\xi) - \langle\kappa(\xi)\rangle$ is killed by 2. The second problem is that in the proof of Lemma 4.5, $\langle cc', dd'\rangle_w$ need not be trivial at real $w$; but in any case $2\langle cc', dd'\rangle_w = 0$. Finally, in our proof of Lemma 4.6, we showed that $\langle\pi, d\rangle_v = 0$ when $\mu_n \subset K$ by instead showing that $2\langle\pi, d\rangle_v = 0$; if $n$ is even, of course, this is insufficient.

Suppose we undertake our construction anyway, yielding $\eta \in \mathrm{H}^1(K, E[n])$. The three problems above imply that our calculation of $\operatorname{Ob}(\eta)$ may be off by an element of $(\operatorname{Br} K)[2]$. If $\ell \geq 4$, then the difference is immaterial, and the proof works. We now consider the cases $\ell = 1$ and $\ell = 2$.

Assume that $\ell = 1$. According to our main theorem, we are under the weakened hypothesis that either $\mu_{2n} \subset K$ or $E$ contains a Galois-stable cyclic subgroup of order $2n$. Using the construction from the previous section, we can come up with a curve $X'$ with period $2n$ and index either $2n$ or $4n$, though we are not able to determine which of the two holds. Suppose $\eta \in \mathrm{H}^1(K, E[2n])$ represents $X'$ with

$\mathrm{Ob}_{2n}(\eta) \in (\mathrm{Br}\, K)[2]$. Let $X$ be the curve with class $2\eta$. Note that we may view $2\eta$ as an element of $\mathrm{H}^1(K, E[n])$; in particular, $X$ has period $n$. To show that $X$ has index $n$, it suffices to show that $\mathrm{Ob}_n(2\eta) = 0$. But by Proposition 2.7, $\mathrm{Ob}_n(2\eta) = 2\,\mathrm{Ob}_{2n}\,\eta = 0$.

The procedure for $\ell = 2$ is similar: construct $X'$ as before with period $2n$ and index $8n$, so that $\mathrm{Ob}_{2n}(\eta)$ has order 4. Then $\mathrm{Ob}_n(2\eta)$ has order 2, and the curve $X$ represented by $2\eta$ has period $n$ and index $2n$.

## 6. Final remarks

The hypothesis on the main theorem amounts to a statement about the Galois representation on $E[n]$. The hypothesis is needed at precisely one place: the calculation of $\langle \pi, d\rangle_v$ appearing in the proof of Lemma 4.6. Recall that $d$ is a product of the conjugates of $\pi$, each appearing with some multiplicity. If one could, for example, choose $\pi$ so that $\langle \pi, \sigma\pi\rangle = 0$ for all $\sigma$, then one could generalize the theorem to arbitrary number fields.

One can get around this to some extent, at least when we wish the index to be maximal ($I = P^2$); see [4], which deals with this case over arbitrary number fields.

The results of the paper should generalize to function fields, that is, finite extensions of $\mathbb{F}_p(T)$. The only wrinkle occurs when $p \mid n$, for then $E[n]$ is no longer an étale group scheme. Clark, in a personal communication, has results making use of a so-called flat Hilbert symbol. One suspects that, with greater care, the results of this paper can be duplicated using the flat symbol.

Lastly, the description of the $\mathrm{Gal}(L/K)$ action on $\mathrm{H}^1(L, E[n])$ yields an explicit description, in most cases, of $\mathrm{H}^1(K, E[n])$ for $K$ an arbitrary number field, in the following manner. Given $E/K$, for $n$ not divisible by a finite set of primes, we know that $\mathrm{Gal}(L/K)$ surjects onto $\mathrm{Aut}(E[n])$. One can show that $\mathrm{H}^q(L/K, E[n]) = 0$ for all $q$, whence the inflation-restriction sequence yields an isomorphism

$$\mathrm{H}^1(K, E[n]) = \mathrm{H}^1(L, E[n])^{\mathrm{Gal}(L/K)}.$$

From Proposition 4.3, one obtains the desired description of $\mathrm{H}^1(K, E[n])$ as pairs of elements of $L^\times / L^{\times n}$.

## References


[1] J. Cassels, *Arithmetic on curves of genus 1. V. Two counterexamples*, J. London Math. Soc. **41** (1966), 244–248.

[2] Pete Clark, *The period-index problem in WC-groups I: elliptic curves*, J. Number Theory **114** (2005), 193–208.

[3] ———, *There are genus one curves of every index over every number field*, J. Reine Angew. Math. **594** (2006), 201–206.

[4] Pete Clark and Shahed Sharif, *Period, index, and the Tate-Shafarevich group of elliptic curves*, In preparation.

[5] Pete L. Clark, *On the indices of curves over local fields*, Manuscripta Math. **124** (2007), no. 4, 411–426. MR MR2357791 (2008m:11121)

[6] Cristian González-Avilés, *Brauer groups and Tate-Shafarevich groups*, J. Math. Sci. Univ. Tokyo **10** (2003), 391–419.

[7] Alexander Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, pp. 88–188. MR 39 #5586c

[8] Serge Lang and John Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684.

[9] Stephen Lichtenbaum, *The period-index problem for elliptic curves*, Amer. J. of Math. **90** (1968), 1209–1223.
[10] ______, *Duality theorems for curves over p-adic fields*, Invent. math. **7** (1969), 120–136.
[11] Qing Liu, Dino Lorenzini, and Michel Raynaud, *Néron models, Lie algebras, and reduction of curves of genus one*, Invent. Math. **157** (2004), 455–518.
[12] ______, *On the Brauer group of a surface*, Invent. Math. **159** (2005), no. 3, 673–676.
[13] David Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354. MR 0204427 (34 #4269)
[14] ______, *Abelian varieties*, Oxford University Press, Oxford, 1985.
[15] Catherine O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory **95** (2002), 329–339.
[16] ______, *Erratum to the period-index obstruction for elliptic curves*, J. Number Theory **109** (2004), 390.
[17] Jean-Pierre Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 82e:12016
[18] Shahed Sharif, *Curves with prescribed period and index over local fields*, J. Algebra **314** (2007), no. 1, 157–167.
[19] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original. MR 95m:11054
[20] William Stein, *There are genus one curves over $\mathbb{Q}$ of every odd index*, J. Reine Angew. Math. **547** (2002), 139–147.
[21] Jakob Stix, *On the period-index problem in light of the section conjecture*, arXiv:math-nt/0802.4125v1, 2008.
[22] Yuri Zarhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15** (1974), 415–419.

Dept. of Mathematics, Duke University, Durham, NC 27708
*E-mail address*: `sharif@math.duke.edu`